[redacted]

Coordinated Science Laboratory

UNIVERSITY OF ILLINOIS - URBANA, ILLINOIS

A THEOREM ON THE MINIMUM DISTANCE OF BCH CODES OVER GF(q)

Vincent Lum

REPORT R-281 MARCH, 1966

This work was supported in part by the Joint Services Electronics Programs (U. S. Army, U. S. Navy, and U. S. Air Force) under Contract No. DA 28 043 AMC 00073(E).

Portions of this work were also supported by the National Science Foundation under Grant NSF GK-690.

A THEOREM ON THE MINIMUM DISTANCE OF BCH CODES OVER GF(q)

Vincent Lum

Abstract

This paper presents a generalization of Mattson-Solomon method for finding the minimum distance of a class of BCH codes. The theorem derived makes it possible to determine fairly easily if a particular code over GF(q) satisfies the conditions set forth and hence has minimum distance exceeding the BCH bound. Application of the theorem is given and numerous examples are presented.

ACKNOWLEDGMENT

The author wishes to express his gratitude to Professor R. T. Chien for his invaluable advice, suggestions and encouragement throughout the period of research for this report.

He would also like to thank his colleague, David Chow, for his constructive criticisms and helpful discussions. Special thanks are extended to Mrs. Divona Keel for her preparation of this manuscript.

A THEOREM ON THE MINIMUM DISTANCE OF BCH CODES OVER GF(q)

I. Introduction

It is well known that many BCH codes have minimum distances greater than those given by the BCH bound. However, little theory has been developed to indicate the conditions necessary in order that a code would have this property. Mattson and Solomon[1] in their paper showed that if a code, defined over GF(2) of length n where $x^n-1 = (x-1)f_1(x)f_2(x)$, $f_i(x)$ irreducible over GF(2), has $\beta,\beta^2,\ldots,\beta^{d_o-1}$ among the roots of its generating polynomial (β primitive n^{th} root of unity), then under certain other conditions, the minimum distance of the code exceeds the BCH bound d_o. This paper represents a generalization of their approach in three different directions: (1) the code being defined over GF(q) where q is power of a prime p, (2) using broader definition of a BCH code, and (3) for a more general n. It will be seen that the generalization is indeed non-trivial and that it is necessary in order to apply to other well-known codes, e.g. the perfect Golay (11,6) code over GF(3). Most of the original Mattson-Solomon results are special case of this general result.

II. Background and Notation

For convenience of the readers we shall present here some of the well-known materials detailed in Mattson-Solomon[1]. This will make the note fairly self-contained. Before we go any further, we should point out that throughout the rest of this note, the correspondence between a code vector and a polynomial is that if a codeword $a = (a_o,a_1,\ldots,a_{n-1})$, then $a(x) = a_o x^{n-1} + a_1 x^{n-2} + \ldots + a_{n-2}x + a_{n-1}$. This may not be the usual correspondence elsewhere.

Consider a sequence $a_o, a_1, \ldots$ in GF(q) = F (q = power of a prime p) defined by the recursion

$$a_{k+i} + b_1 a_{k+i-1} + \ldots + b_k a_i = 0 \quad i = 0,1,2,\ldots \tag{1}$$

where $b_i \in GF(q)$ are known. If $a_o, a_1, \ldots, a_{k-1}$ are given, then all other a_i can be computed. The general solution is found by letting $a_j = \beta^j$, obtaining

$$\beta^i(\beta^k + b_1\beta^{k-1} + \ldots + b_{k-1}\beta + b_k) = 0 \quad .$$

If β is a root of $f(x) = x^k + b_i x^{k-1} + \ldots + b_{k-1}x + b_k$, the equation will be satisfied. We shall assume f(x) has no repeated roots.

Let K be an extension field of GF(q) which contains all the roots of $x^n - 1$, denoted by $\beta_1, \beta_2, \ldots, \beta_k$. Let

$$a_j = c_1\beta_1{}^j + c_2\beta_2{}^j + \ldots + c_k\beta_k{}^j \qquad j = 0,1,2,\ldots$$

with $c_i \in K$. Given a set of values of $a_o, a_1, \ldots, a_{k-1}$, there is a unique set of $c_1, c_2, \ldots, c_k$ such that this equation is true. Thus we have the following lemma.

Lemma 1 (Mattson-Solomon). If $a_o, a_1, \ldots$ is a sequence in F given by the recursion of (1) and if the polynomial $f(x) = x^k + b_1 x^{k-1} + \ldots + b_k$ has no repeated roots, then there exist uniquely determined elements $c_1, c_2, \ldots, c_k$ in K such that

$$a_j = c_1\beta_1{}^j + \ldots + c_k\beta_k{}^j \qquad j = 0,1,2,\ldots$$

where $\beta_1, \beta_2, \ldots, \beta_k$ are roots of f(x).

Consider an integer n where n and p are relatively prime. Let $f(x) = x^k + b_1 x^{k-1} + \ldots + b_k$ with $b_i \in GF(q)$ be a factor of x^n-1. Take f(x) as the recursion polynomial of a code A with length n and information digits k. Then Equation (1) is the definition of a code.

Definition 1: Let V be a vector space of n-tuples. Then the code A attached to f(x) is given by

$$A = \{a \mid a = (a_o a_1 \ldots a_{n-1}) \in V,$$

$$a_{k+i} + b_1 a_{k+i-1} + \ldots + b_k a_i = 0,$$

$$i = 0,1,\ldots,n-k-1\} .$$

Definition 2: Let β be a primitive n^{th} root of unity over GF(q). Let $\beta^{m_o}, \beta^{m_o+1}, \ldots, \beta^{m_o+d_o-2}$ be roots of generating polynomial g(x) where $g(x)f(x) = x^n-1$. Then the code attached to f(x) as defined by Definition 1 is BCH code.

It is implicitly assumed that neither β^{m_o-1} nor $\beta^{m_o+d_o-1}$ is a root of g(x) so that the BCH bound of the code so defined is d_o. We shall use d_o to denote BCH bound in the rest of this paper. The BCH codes defined in Mattson-Solomon has $m_o = 1$ always.

Definition 3: Let $f(x) \in F[x]$ and $f(x) \mid x^n-1$ where (n,p) = 1. Let β be a primitive n^{th} root of unity. Define

$$E(\beta) = \{0 \leq e \leq n-1,\ f(\beta^e) = 0\}$$

and if m is an arbitrary integer, define

$$E'(\beta) = \{0 \leq e' \leq n-1,\ f(\beta^{m+e'}) = 0\}$$

and call m the integer associated with $E'(\beta)$. Moreover, we let $e_i \equiv m + e_i' \mod n$.

It is obvious that the set of integers in $E(\beta)$ is congruent modulo n to the set in $E'(\beta)$. The knowledge of this fact is very useful in the proofs of following theorems.

Lemma 2 (Mattson-Solomon). For each $a = (a_0,\ldots,a_{n-1}) \in A$ there is a polynomial $g_a(x) = c_1x^{e_1} + c_2x^{e_2} + \ldots + c_kx^{e_k}$ with $c_i \in K$ such that $a_i = g_a(\beta^i)$ for $i = 0,1,\ldots,n-1$. β being fixed, this polynomial is uniquely determined by a. The degree of $g_a(x)$ is at most e, the largest integer in $E(\beta)$. Proof of this lemma is given in Mattson-Solomon[1].

Corollary 1: For each $a \in A$, there exists a polynomial $p_a(x)$ with coefficients in $K \geq F$ such that

$$p_a(x) = c_1x^{e_1'} + c_2x^{e_2'} + \ldots + c_kx^{e_k'}$$

and

$$a_i = \beta^{mi}\, p_a(\beta^i) \qquad i = 0,1,\ldots,n-1$$

where $e_1',e_2',\ldots,e_k'$ are elements of $E'(\beta)$ and m an integer associated with $E'(\beta)$. Furthermore, the coefficients $c_1,\ldots,c_k$ are some as those in $g_a(x)$.

Proof: From definition of $E(\alpha)$ and Lemma 1,

$$a_i = c_1(\beta^{e_1})^i + c_2(\beta^{e_2})^i + \ldots + c_k(\beta^{e_k})^i$$

The c_i's for $i = 1,2,\ldots,k$ are actually coefficients of $g_a(x)$ given in Lemma 2.

By definition of $E'(\beta)$ and m, we also have

$$\begin{aligned} a_i &= c_1(\beta^{m+e_1'})^i + c_2(\beta^{m+e_2'})^i + \ldots + c_k(\beta^{m+e_k'})^i \\ &= \beta^{mi}\,[c_1(\beta^i)^{e_1'} + c_2(\beta^i)^{e_2'} + \ldots + c_k(\beta^i)^{e_k'}] \\ &= \beta^{mi}\, p_a(\beta^i) \end{aligned}$$

where $p_a(x) = c_1 x^{e_1'} + c_2 x^{e_2'} + \ldots + c_k x^{e_k'}$.

III. Results and Discussion

The technique used in the proof of Corollary 1 though simple is very effective in generalizing Mattson-Solomon approach[1]. It is obvious that $p_a(x)$ due to its definition has the same set of roots as $g_a(x)$ has over the set of all n^{th} roots of unity denoted by U. Thus the number of roots $p_a(x)$ possesses in U defines the number of zero components of a codeword $a \in A$. By suitable choice of m, we shall show using the new method that the code defined by Definition 2 has minimum distance at least equal to the BCH bound.

Theorem 1: Let the BCH code be defined as in Definition 2. Then the minimum distance of the code is $d \geq d_o$.

Proof: From Definition 2, we know that $\beta^{m_o}, \beta^{m_o+1}, \ldots, \beta^{m_o+d_o-2}$ are roots of the generating polynomial g(x). If we let

$$m \equiv m_o - (n-d_o+1) \pmod{n}$$

where m is an integer associated with $E'(\beta)$, then we have

$$\beta^{m_o} = \beta^{m+(n-d_o+1)}$$

$$\beta^{m_o+1} = \beta^{m+(n-d_o+2)}$$

$$\vdots$$

$$\beta^{m_o+d_o-2} = \beta^{m+(n-1)}$$

With the m so chosen, we guarantee that $n-d_o+1, n-d_o+2, \ldots, n-1$ are not elements of $E'(\beta)$. Thus the largest possible integer in $E'(\beta)$ is $n-d_o$, and so $p_a(x)$

can have at most $n-d_o$ roots in U. The minimum weight of the code must therefore be $d \geq d_o$.*

Consider now a class of BCH codes over GF(q) with code lenth n being odd prime. Under this condition x^n-1 will have irreducible factors all of same degree except the trivial factor $(x-1)$. Let

$$x^n-1 = (x-1)f_1(x)f_2(x)\ldots f_t(x) \qquad (2)$$

where $f_i(x)$, $i = 1,2,\ldots,t$ are irreducible over GF(q) and each of degree h. Furthermore we require that the coefficients of the $(h-1)$-degree term are distinct for at least two of the polynomials among $f_1(x), f_2(x), \ldots, f_t(x)$. Denote these two polynomials by $f_r(x)$ and $f_s(x)$. The codes that we shall consider are the $(n,h+1)$ codes over GF(q) satisfying the conditions just given. Consequently the recursion polynomial of these codes will be in the form of

$$f(x) = (x-1)f_a(x), \qquad 1 \leq a \leq t$$

If we let β^{e_1}, $e_1 \neq 0$, denote a root of f(x), then $(\beta^{e_1})^q, (\beta^{e_1})^{q^2}, \ldots, (\beta^{e_1})^{q^{h-1}}$ are also roots of f(x) and these are distinct. Furthermore these roots and unity represent all the roots of f(x). (For proof of this statement, see Peterson[2] Theorem 6.21 and 6.26). Applying this result to definition of $E(\beta)$, we have $E(\beta) = \{0, e_1, e_2, \ldots, e_h\}$ where

$$e_j \equiv q^{j-1}e_1 \pmod{n} \quad \text{for } e_1, e_j \in E(\beta);\ e_1 e_j \neq 0$$

and

$$q^h \equiv 1 \pmod{n}$$

---

*It was learned after the completion of this work that E. F. Assmus and H. F. Mattson have obtained independently similar results, to be published in the Proceedings of the Royan "Summer School."

and no $h' < h$ will satisfy this relation. We shall now present a generalized version of a lemma due to Reed[3].

Lemma 3: Let $F = GF(q)$ be a finite field and K an extension of F. Let $h(x) = c_o + c_1 x + \ldots + c_k x^k$ be any polynomial in $K[x]$. Let β be a primitive n^{th} root of unity in K, $n \not\equiv 0 \ (p)$. If degree of $h(x) < n$, then

$$nc_j = \sum_{i=0}^{n-1} h(\beta^i)\beta^{-ji}$$

where n is to be taken as n modulo p, and p is characteristic of the field F.

Proof:

$$h(\beta^i) = c_o + c_1\beta^i + c_2(\beta^i)^2 + \ldots + c_k(\beta^i)^k$$

$$h(\beta^i)\beta^{-ji} = [c_o + c_1\beta^i + c_2(\beta^2)^i + \ldots + c_k(\beta^k)^i]\beta^{-ji}$$

$$\sum_{i=0}^{n-1} h(\beta^i)\beta^{-ji} = h(\beta^o) + h(\beta)\beta^{-j} + h(\beta^2)\beta^{-2j} + \ldots + h(\beta^{n-1})\beta^{-j(n-1)}$$

$$= c_o(1 + \beta^{-j} + (\beta^j)^2 + \ldots + (\beta^j)^{n-1})$$

$$+ c_1(1 + \beta^{1-j} + (\beta^{1-j})^2 + \ldots + (\beta^{1-j})^{n-1})$$

$$+ \ldots$$

$$+ c_k(1 + \beta^{k-j} + (\beta^{k-j})^2 + \ldots + (\beta^{k-j})^{n-1})$$

Noting that $1 + \alpha + \alpha^2 + \ldots + \alpha^{n-1} = \frac{1-\alpha^n}{1-\alpha}$, we get

$$\sum_{i=0}^{n-1} h(\beta^i)\beta^{-ji} = \sum_{k\neq j} c_k \sum_{i=0}^{n-1} \beta^{i(k-j)} + c_j \sum_{i=0}^{n-1} 1$$

$$= \sum_{k\neq j} c_k \frac{1-(\beta^{k-h})^n}{1-\beta^{k-j}} + nc_j = nc_j$$

since β is primitive n^{th} root of unity.

Lemma 4: Let $g_a(x) = c_o + c_1 x^{e_1} + c_2 x^{e_2} + \ldots + c_h x^{e_h}$ for a given $a \in A$. Then

$$nc_o = \sum_{i=0}^{n-1} a_i$$

and

$$nc_j = \sum_{i=0}^{n-1} a_i \beta^{-e_j i}$$

Furthermore, $c_o^q = c_o$, $c_1^q = c_2$, $c_2^q = c_3$, $\ldots$, $c_h^q = c_1$.

Proof: The first part of the lemma is a direct result of Lemma 3. For the second part, we recall that

$$e_j \equiv q^{j-1} e_1 \pmod{n}$$

and

$$q^h \equiv 1 \pmod{n}$$

$$c_o^q = c_o \quad \text{since } c_o \in GF(q)$$

$$(nc_j)^q = \left(\sum_{i=0}^{n-1} a_i \beta^{-e_j i} \right)^q = \sum_{i=0}^{n-1} a_i \beta^{-q e_j i}$$

$$= \sum_{i=0}^{n-1} a_i \beta^{-e_{j+1} i} = nc_{j+1}$$

With the preliminary theory thus set up, we are now ready to state and prove the main theorem.

Theorem 2: Let $a \in A$ over $GF(q)$ have

$$g_a(x) = c_o + c_1 x^{e_1} + c_2 x^{e_2} + \ldots + c_h x^{e_h}$$

and

$$p_a(x) = c_o x^{e_o'} + c_1 x^{e_1'} + c_2 x^{e_2'} + \ldots + c_h x^{e_h'}$$

as defined before. Let the leading coefficient of $p_a(x)$ be c_k and the constant term be $c_k^{q^i}$. If $(i,h) = 1$ and $d_o < h$, then the code has minimum distance $\geq d_o + 1$. If either the constant term or the leading coefficient of $p_a(x)$ is c_o, and $d_o < h$, then the code has minimum distance $\geq d_o + 1$.

Proof: First let us prove the first part of the theorem. We have

$$p_a(x) = c_o x^{e_o'} + c_1 x^{e_1'} + \ldots + c_h x^{e_h'}$$

$$= c_k (c_k^{q^i-1} + c_{i_1} x^{e_{i_1}'} + \ldots + x^{e_k'})$$

where the highest degree term is $x^{e_k'}$. By suitable choice of m associated with $E'(\beta)$ as is done in the proof of Theorem 1, we know that $e_k' \leq n-d_o$. Furthermore, by definition of BCH code and Theorem 1, we know actually $e_k = n-d_o$. We shall now assume that the minimum distance of the code is d_o and show a contradiction.

Suppose minimum distance of the code is d_o. Then $c_k^{q^i-1}$ is a product of $n^{\underline{th}}$ roots of unity and therefore

$$(c_k^{q^i-1})^n = 1$$

$$(c_k^n)^{q^i} = (c_k^{q^i})^n = (c_k^{q^i-1} \cdot c_k)^n = c_k^n$$

This implies c_k^n is an element of the field $GF(q^i)$. Rewriting $g_a(x)$ in terms of c_k in the coefficients, we have

$$g_a(x) = c_o + c_k x^{e_k} + (c_k x^{e_k})^q + \ldots + (c_k x^{e_k})^{q^{h-1}}$$

We know that $c_k \neq 0$, otherwise $a \in A$ corresponding to this $g_a(x)$ is either the zero vector or the all 1's vector. We also know that $n \mid q^h-1$ but

$n \nmid q^{h'}-1$ for any $h' < h$. From the way the coefficients of $g_a(x)$ are defined, we have $i < h$. Thus $n \nmid q^i-1$. n being a prime implies $(n,q^i-1) = 1$. Thus

$$\{q^n, q \in GF(q^i)\} = \{q, q \in GF(q^i)\}$$

$GF(q^i)$ being a field and c_k and element in it implies that there exists a $q_1 \in GF(q^i)$ such that $q_1 c_k^{\,n} = 1$, $q_1 \neq 0$. But the relation just stated implies that there is a $q_o \in GF(q^i)$ such that $q_o^{\,n} = q_1$. We therefore obtain $(q_o c_k)^n = 1$ and so $q_o c_k$ is a $n^{\underline{th}}$ root of unity. Hence $q_o c_k \beta^{e_k j}$ is a $n^{\underline{th}}$ root of unity.

Since $q_o \neq 0$, $a_j \neq 0$ implies $q_o a_j \neq 0$

$$q_o a_j = q_o g_a(\beta^j)$$

$$= q_o c_o + q_o c_k \beta^{e_k j} + q_o (c_k \beta^{e_k j})^q + \ldots + q_o (c_k \beta^{e_k j})^{q^{h-1}}$$

Since $(i,h) = 1$, there exists integers w and v such that $iw + hv = 1$. Thus for $\ell = 1,2,\ldots,h-1$, we have w_ℓ, v_ℓ such that $iw_\ell + hv_\ell = \ell$. Thus

$$q_o (c_k \beta^{e_k j})^{q^\ell} = q_o (c_k \beta^{e_k j})^{q^{iw_\ell + hv_\ell}}$$

$$= q_o [(c_k \beta^{e_k j})^{q^{iw_\ell}}]^{q^{hv_\ell}} = q_o (c_k \beta^{e_k j})^{q^{iw_\ell}}$$

$$= (q_o c_k \beta^{e_k j})^{q^{iw_\ell}} \qquad \text{since } q_o \in GF(q^i)$$

$$\text{and } q_o^{\,q^i} = q_o$$

Now $q_o a_j$ becomes

$$q_o a_j = q_o c_o + q_o c_k \beta^{e_k j} + q_o (c_k \beta^{e_k j})^{q^{iw_1}} + \ldots + q_o (c_k \beta^{e_k j})^{q^{iw_{h-1}}}$$

$$= q_o c_o + q_o c_k \beta^{e_k j} + (q_o c_k \beta^{e_k j})^{q^{iw_1}} + \ldots + (q_o c_k \beta^{e_k j})^{q^{iw_{h-1}}}$$

Now since $(e_k, n) = 1$, $\beta^{e_k j}$ will take on all values of n^{th} root of unity as j runs from 0 to n-1. This implies $q_o c_k \beta^{e_k j}$ will generate the set of all n^{th} roots of unity for $j = 0,1,\ldots,n-1$. For h times $q_o c_k \beta^{e_k j}$ will be a root of $f_r(x)$ and thus

$$q_o c_k \beta^{e_k j} + (q_o c_k \beta^{e_k j})^{q^{iw_1}} + \ldots + (q_o c_k \beta^{e_k j})^{q^{iw_{h-1}}}$$

is the coefficient of the (h-1)-degree term. For h times this sum is coefficient of that same degree term in $f_s(x)$. Since these coefficients are assumed to be different $q_o a_j$, and so a_j, must be nonzero at least h times. This contradicts the assumption that minimum distance is $d_o < h$. Hence the code has minimum distance $\geq d_o + 1$.

Now we shall prove the second part of the theorem. The constant term or leading coefficient of $p_a(x)$ being c_o implies that either $\frac{c_o}{c_k}$ or $\frac{c_k}{c_o}$ being a product of n^{th} root of unity and thus $\frac{c_o}{c_k}$ or $\frac{c_k}{c_o}$ a n^{th} root of unity. (We assume c_k being either leading coefficient or constant term depending on the case of c_o). In either case we have

$$\left(\frac{c_k}{c_o}\right)^n = 1 \text{ or } c_o^{\,n} = c_k^{\,n}$$

$c_o \neq 0$ for otherwise the theorem is true already. Therefore $c_k^n \in GF(q)$. For the same reason as that shown in the proof of the first part of this theorem, there exist q_o and q_1 in GF(q) such that $q_1 = q_o^n$ and $q_1 c_k^n = (q_o c_k)^n = 1$. Now we have again as before

$$q_o a_j = q_o g_a(\beta^j)$$

$$= q_o c_o + q_o c_k \beta^{e_k j} + q_o (c_k \beta^{e_k j})^q + \ldots + q_o (c_k \beta^{e_k j})^{q^{h-1}}$$

$$= q_o c_o + q_o c_k \beta^{e_k j} + (q_o c_k \beta^{e_k j})^q + \ldots + (q_o c_k \beta^{e_k j})^{q^{h-1}}$$

The remaining of the proof is exactly same as that of the first part just given and we arrive at same contradiction. The proof is thus complete.

Let b_i denote the coefficient of the (h-1)-degree term of $f_i(x)$ which is an irreducible factor of x^n-1 over GF(q) and is not equal to (x-1). From Equation (2) we have t number of b_i's which may not be distinct. Let b_s occur the least often in this set and let it occur w times. With this notation, we have the following corollary.

Corollary 2: Let all conditions be same as those in Theorem 2 except the part relating to the BCH bound changed to the following: If $d_o < wh$, then minimum distance of code $\geq d_o + 1$. Proof is obvious from proof of Theorem 2.

In the special case that q = 2 and c_o is either leading coefficient or a constant term, the same technique given in Mattson-Solomon[1] may be used so that the distance may be increased to $d_o + 2$ in some cases. This technique unfortunately cannot apply to the general case $q \neq 2$.

In attempting to use the above technique on a more general n, not a prime, and on a code whose recursion polynomial contains more than one $f_i(x)$, $i = 1,2,\ldots,t$ and $f_i(x) \neq x-1$, one encounters much difficulty. One major problem lies in the lack of explicit relation among the coefficients c_i's of $g_a(x)$. However, for a limited case of n not a prime but the recursion polynomial still has only one factor besides $(x-1)$, we can apply the above technique successfully.

Let x^n-1, where n is not a prime, be factored over GF(q) into irreducible polynomials $f_i(x)$, $i = 1,2,\ldots,t$ and $f_i(x) \neq x-1$. Let the recursion polynomial of the code be given by $f(x) = (x-1)f_a(x)$, $1 \leq a \leq t$, where $f_a(x)$ is of degree h and belongs to exponent n. We further require that there exists $f_b(x)$ among the set $\{f_i(x), i = 1,2,\ldots,t\}$ such that $f_b(x)$ has also degree h and belongs to the exponent n, but its coefficient of the $(h-1)$-degree term differs from that of $f_a(x)$. Under such conditions, the following theorem can be applied to this (n,h+1) code.

Theorem 3: Let the (n,h+1) code be as defined above. Let $a \in A$ define $g_a(x)$ and $p_a(x)$ as in Lemma 1 and Corllary 1. Suppose e_m = minimum nonzero value of $E(\beta)$ is relatively prime to n. Let the leading coefficient of $p_a(x)$ be c_k and the constant term be $c_k^{q^i}$. If $(i,h) = 1$, $(n,q^i-1) = 1$ and $d_o < h$, then the minimum distance of the code $\geq d_o + 1$. If either the constant term or leading coefficient of $p_a(x)$ is c_o, and if $(n,q-1) = 1$ and $d_o < h$, then the code has minimum distance $\geq d_o + 1$.

Proof: The proof is exactly the same as that of Theorem 2. However, we shall point out the following details.

It is noted that when n is not prime we need to insert several constraints. The condition that $(e_m,n) = 1$ is necessary to guarantee that the set of

$\{q_o c_k \beta^{e_k j}, j = 0,1,\ldots,n-1\}$ will take all values of the n^{th} roots of unity. Note that $e_k = q^i e_m$ for $e_k \neq 0$ and $e_k \in E(\beta)$, i an integer since $(q,n) = 1$, $(e_m,n) = 1$ implies $(e_k,n) = 1$ for all nonzero $e_k \in E(\beta)$. $(q,n) = 1$ because assumed condition x^n-1 has no multiple roots.

The second condition $(n,q^i-1) = 1$ is required so that for every $q_1 \in GF(q^i)$, there exists $q_o \in GF(q^i)$ such that $q_o^n = q_1$. When n is a prime, this condition is automatically satisfied. The application of this condition is obvious when reading the proof of Theorem 2.

Finally, the third condition $(n,q-1)$ is used in exactly the same way as the second but it occurs in the proof of the second half of the theorem. Applying these conditions to the proof of Theorem 2, we will have the proof of Theorem 3.

We can generalize the theorem a little further as we have done in Corollary 2. However, because it will be so similar to Corollary 2 that we shall not write it as an explicit corollary, but we must bear this in mind when applying this theorem.

IV. Examples of Application

With the theory now completed, we can proceed to illustrate the application of the theorems. Since the results of Mattson-Solomon are special case of this general theory, their examples can naturally be used here as well. As they have illustrated in detail how the minimum distance of those codes can be found to be larger than the BCH bound, we shall not delve on them any further. Instead, we shall show a few more interesting codes in which the theory is applicable.

First, consider the (73,10) code over GF(2). It was found that $x^{73}-1 = (x-1)f_1(x)f_2(x)\ldots f_8(x)$ where $f_i(x)$, $i = 1,2,\ldots,8$ are irreducible

over GF(2) and each one is of degree 9. The BCH bound for this code is $d_o = 25$ and $m_o = 1$. Among the factors $f_i(x)$, $i = 1,\ldots,8$, we have five coefficients of the $8^{\underline{th}}$-degree term are 0's and three of these are 1's. Thus $w = 3$ and $wh = 3 \cdot 9 = 27$. Hence $d_o = 25 < 27$ and Corollary 2 states the code has minimum distance $d \geq 25 + 1 = 26$. But if $d = 26$, then $c_o = 0$. For this code, we have $E(\beta) = \{0,25,50,27,54,35,70,67,61,49\}$, β primitive $73^{\underline{th}}$ root of unity, and for any codeword a,

$$g_a(x) = c_o + c_1x^{25} + c_2x^{50} + c_3x^{27} + c_4x^{54} + c_5x^{35} + c_6x^{70} + c_7x^{67} + c_8x^{61} + c_9x^{49}$$

$c_o = 0$ implies

$$g_a(x) = x^{25}(c_1 + c_2x^{25} + c_3x^2 + \ldots + c_6x^{45} + \ldots + c_0x^{24})$$

which can have at most 45 zeros in U, the set of $73^{\underline{th}}$ roots of unity. This says that weight of a is 28. Contradiction. Hence this code has minimum distance ≥ 27.

The perfect Golay (11,6) code over GF(3) is a very illuminating example for the nonbinary case and $m_o \neq 1$. However, this code has been worked out completely in Chien-Lum[4] and therefore will not be given here. Instead we shall take a brief look at the (19,10) code over GF(4). We have in this case

$$E(\beta) = \{0,2,8,13,14,18,15,3,12,10\}$$

We have in this case $m_o = 4$, $d_o = 5$ and $h = 9$. (Note that if m_o is taken to be 1, then d_o is only 2). Defining m associated with $E'(\beta)$ as in the proof of Theorem 1, we have

$$m \equiv m_o - (n-d_o+1) \qquad \text{mod } n$$

$$\equiv 4 - (19-5+1) \qquad \text{mod } 19$$

$$\equiv 8 \qquad \text{mod } 19$$

Thus obtaining $E'(\beta) = \{11,13,0,5,6,10,7,14,4,2\}$ and

$$p_a(x) = c_o x^{11} + c_1 x^{13} + c_2 + c_3 x^5 + c_4 x^6 + c_5 x^{10}$$

$$+ c_6 x^7 + c_7 x^{14} + c_8 x^4 + c_9 x^2$$

The constant term is c_2 and the leading coefficient is c_7. By Lemma 4, we have $c_7^{4^4} = (c_7^{4^3})^4 = c_1^4 = c_2$. Since $(4,9) = 1$ and $d_o = 5 < h = 9$, the conditions of Theorem 2 are satisfied. There is however one more condition to be checked, namely, that the coefficients of the $8^{\underline{th}}$-degree terms in the nontrivial factors of $x^{19}-1$ are different. Since $x^{19}-1 = (x-1) f_1(x) f_2(x)$, $f_1(x)$ and $f_2(x)$ are irreducible over GF(4), those two coefficient must be different as the characteristic of the field is 2. Now all constraints are met, and by Theorem 2, the minimum distance of the code must be $\geq d_o + 1 = 6$.

Other results are obtained in similar manner. In many cases, some of the conditions are met automatically. Such is the case for h being a prime; for then $(i,h) = 1$ is always satisfied. Short cuts like this can be observed in calculations. The following table contains some of the codes for which the theorems apply.

Table I

Table of Codes for Which the Theory Applies

Base field	n	k	Total no. of irreducible factors of x^n-1	m_o	h	d_o	min. distance $d \geq$
GF(2)	17	9	3	5	8	4	5
	23	12	3	1	11	5	7
	43	15	4	1	14	7	9
	47	24	3	1	23	5	7
	71	36	3	1	35	7	9
	73	10	9	1	9	25	27
	113	29	5	33	28	17	18
	151	16	11	1	15	37	39
GF(3)	11	6	3	3	5	4	5
GF(4)	11	6	3	3	5	4	5
	19	10	3	4	9	5	6
	23	12	3	1	11	5	6
	47	24	3	1	23	5	6
	29	15	3	4	14	5	6
GF(5)	11	6	3	3	5	4	5

V. Conclusion

It is demonstrated in this paper that the approach of Mattson-Solomon[1] can be generalized fruitfully to BCH codes defined over GF(q) with less restriction on the code length. That the generalization is nontrivial can be seen from the introduction of a number of new concepts as illustrated in the steps leading to the main theorem (Theorem 2 in this paper).

It is also apparent that the new result leads to a much larger class of BCH codes than known before. With some labor of hand computation we have succeeded in obtaining the codes listed in Table I. It is believed that more extensive tables are easily obtainable with the aid of a digital computer.

References

1. H. F. Mattson and G. Solomon, "A New Treatment of Bose-Chaudhuri Codes," SIAM, Vol. 9, December, 1961.

2. W. W. Peterson, Error Correcting Codes, MIT Press, 1961.

3. I. Reed and G. Solomon, "A Decoding Procedure for a Polynomial Code," Group Report 47-37, Lincoln Laboratory, 1960.

4. R. T. Chien and V. Lum,"On Golay's Perfect Codes and Step-by-Step Decoding," to appear in IEEE Trans., PGIT.

Distribution list as of March 1, 1965

1 Dr. Chalmers Sherwin
Deputy Director (Research & Technology)
DD&RE Rm 3E1060
The Pentagon
Washington, D. C. 20301

1 Dr. Edward M. Reilley
Asst. Director (Research)
Ofc. of Defense Res & Eng
Department of Defense
Washington, D. C. 20301

1 Dr. James A. Ward
Office of Deputy Director (Research and Information Rm 3D1037)
Department of Defense
The Pentagon
Washington, D. C. 20301

1 Director
Advanced Research Projects Agency
Department of Defense
Washington, D. C. 20301

1 Mr. Charles Yost, Director
for Materials Sciences
Advanced Research Projects Agency
Department of Defense
Washington, D. C. 20301

20 Defense Documentation Center
Cameron Station, Bldg. 5
Alexandria, Virginia 22314
Attn: TISIA

1 Director
National Security Agency
Fort George G. Meade, Maryland 20755
Attn: Librarian C-332

1 Chief of Research and Development
Headquarters, Department of the Army
Washington, D. C. 20310
Attn: Physical Sciences Division P & E

1 Chief of Research and Development
Headquarters, Department of the Army
Washington, D. C. 20310
Attn: Mr. L. H. Geiger, Rm 34442

1 Research Plans Office
U. S. Army Research Office
3045 Columbia Pike
Arlington, Virginia 22204

1 Commanding General
U. S. Army Materiel Command
Attn: AMCRD-RS-PE-E
Washington, D. C. 20315

1 Commanding General
U. S. Army Strategic Communications Command
Washington, D. C. 20315

1 Commanding Officer
U. S. Army Materials Research Agency
Watertown Arsenal
Watertown, Massachusetts 02172

1 Commanding Officer
U. S. Army Ballistics Research Lab.
Aberdeen Proving Ground
Aberdeen, Maryland 21005
Attn: V. W. Richards

1 Commanding Officer
U. S. Army Ballistics Research Lab.
Aberdeen Proving Ground
Aberdeen, Maryland 21005
Attn: Keats A. Pullen, Jr.

1 Commanding Officer
U. S. Army Ballistics Research Lab.
Aberdeen Proving Ground
Aberdeen, Maryland 21005
Attn: George C. Francis, Computing Lab.

1 Commandant
U. S. Army Air Defense School
P. O. Box 9390
Fort Bliss, Texas 79916
Attn: Missile Sciences Div., C&S Dept.

1 Commanding General
U. S. Army Missile Command
Redstone Arsenal, Alabama 35809
Attn: Technical Library

1 Commanding General
Frankford Arsenal
Philadelphia, Pa. 19137
Attn: SMUFA-1310 (Dr. Sidney Ross)

1 Commanding General
Frankford Arsenal
Philadelphia, Pa. 19137
Attn: SMUFA-1300

1 U. S. Army Munitions Command
Picatinney Arsenal
Dover, New Jersey 07801
Attn: Technical Information Branch

1 Commanding Officer
Harry Diamond Laboratories
Connecticut Ave. & Van Ness St., N.W.
Washington, D. C. 20438
Attn: Mr. Berthold Altman

1 Commanding Officer
Harry Diamond Laboratories
Attn: Library
Connecticut Ave. & Van Ness St., N.W.
Washington, D. C. 20438

1 Commanding Officer
U. S. Army Security Agency
Arlington Hall
Arlington, Virginia 22212

1 Commanding Officer
U. S. Army Limited War Laboratory
Aberdeen Proving Ground
Aberdeen, Maryland 21005
Attn: Technical Director

1 Commanding Officer
Human Engineering Laboratories
Aberdeen Proving Ground, Maryland 21005

1 Director
U. S. Army EngineerGeodesy. Intelligence and Mapping, Research & Devel. Agency
Fort Belvoir, Virginia 22060

1 Commandant
U. S. Army Command and General Staff College
Fort Leavenworth, Kansas 66207
Attn: Secretary

1 Dr. H. Robl, Deputy Director
U. S. Army Research Office (Durham)
Box CM, Duke Station
Durham, North Carolina 27706

1 Commanding Officer
U. S. Army Research Office (Durham)
P. O. Box CM, Duke Station
Durham, North Carolina 27706
Attn: CRD-AA-IP (Richard O. Ulsh)

1 Commanding General
U. S. Army Electronics Command
Fort Monmouth, New Jersey 07703
Attn: AMSEL-SC

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: Dr. S. Benedict Levin, Director
Institute for Exploratory Research

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: Mr. Robert O. Parker, Executive Secretary, JSTAC (AMSEL-RD-X)

1 Superintendent
U. S. Military Academy
West Point, New York 10996

1 The Walter Reed Institute of Research
Walter Reed Army Medical Center
Washington, D. C. 20012

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-DR

1 Director
U. S. Army Electronics Laboratories
Attn: AMSEL-RD-X
Fort Monmouth, New Jersey 07703

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-XE

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-XC

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-XS

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-NR

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-NE

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-NO

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-NP

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-SA

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-SE

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-SR

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-SS

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-PE

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-PF

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-PR

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RL-GF

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-ADT

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-FU#1

1 Commanding Officer
U. S. Army Electronics R&D Activity
Fort Huachuca, Arizona 85163

1 Commanding Officer
U. S. Army Engineers R&D Laboratory
Fort Belvoir, Virginia 22060
Attn: STINFO Branch

1 Commanding Officer
U. S. Army Electronics R&D Activity
White Sands Missile Range
New Mexico 88002

1 Director
Human Resources Research Office
The George Washington University
300 N. Washington Street
Alexandria, Virginia

1 Commanding Officer
U. S. Army Personnel Research Office
Washington 25, D. C.

1 Commanding Officer
U. S. Army Medical Research Laboratory
Fort Knox, Kentucky

1 Commanding General
U. S. Army Signal Center and School
Attn: Chief, Office of Academic Operations
Fort Monmouth, New Jersey 07703

2 Dr. Richard H. Wilcox, Code 437
Department of the Navy
Washington, D. C. 20360

1 Chief, Bureau of Weapons
Attn: Technical Library, DLI-3
Department of the Navy
Washington, D. C. 20360

1 Chief, Bureau of Ships
Department of the Navy
Washington, D. C. 20360
Attn: Code 680

1 Chief, Bureau of Ships
Department of the Navy
Washington, D. C. 20360
Attn: Code 732

1 Commander
U. S. Naval Air Development Center
Johnsville, Pennsylvania
Attn: NADC Library

1 Commanding Officer
Naval Electronics Laboratory
San Diego, California 92052
Attn: Code 2222(Library)

1 Commanding Officer
Naval Electronics Laboratory
San Diego, California 92052
Attn: Code 2800, C. S. Manning

1 Commanding Officer and Director
(Code 142 Library)
David W. Taylor Model Basin
Washington, D. C. 20007

6 Director
Naval Research Laboratory
Washington, D. C. 20390
Attn: Technical Information Office (Code 2000)

1 Commanding Officer
Office of Naval Research Branch Office
219 S. Dearborn Street
Chicago, Illinois 60604

1 Chief of Naval Operations
Department of the Navy
Washington, D. C. 20350
Attn: OP-07T

1 Chief of Naval Operations
Department of the Navy
Washington, D. C. 20350
Attn: OP-03EG

1 Commanding Officer
Office of Naval Research Branch Office
1000 Geary Street
San Francisco, California 94109

1 Commanding Officer
U. S. Naval Weapons Laboratory
Asst. Director for Computation
Dahlgren, Virginia 22448
Attn: G. H. Gleissner (Code K-4)

1 Inspector of Naval Material
Bureau of Ships Technical Representative
1902 West Minnehaha Avenue
St. Paul 4, Minnesota

5 Lt. Col. E. T. Gaines, SREE
Chief, Electronics Division
Directorate of Engineering Sciences
Air Force Office of Scientific Research
Washington, D. C. 20333

1 Director of Science & Technology
Deputy Chief of Staff (R & D)
USAF
Washington, D. C.
Attn: AFRST-EL/GU

1 Director of Science & Technology
Deputy Chief of Staff (R & D)
USAF
Washington, D. C.
Attn: AFRST-SC

1 Karl M. Fuechsel
Electronics Division
Director of Engineering Sciences
Air Force Office of Scientific Research
Washington, D. C. 20333

1 Lt. Col. Edwin M. Myers
Headquarters, USAF (AFRDR)
Washington 25, D. C.

1 Director, Air University Library
Maxwell Air Force Base
Alabama 36112
Attn: CR-4803a

1 Commander
Research & Technology Division
AFSC (Mr. Robert L. Feik)
Office of the Scientific Director
Bolling AFB 25, D. C.

1 Commander
Research & Technology Division
Office of the Scientific Director
Bolling AFB 25, D. C.
Attn: RTHR

1 Commander
Air Force Cambridge Research Laboratories
Attn: Research Library
CRMXL-R
L. G. Hanscom Field
Bedford, Massachusetts 01731

1 Dr. Lloyd Hollingsworth
AFCRL
L. G. Hanscom Field
Bedford, Massachusetts 01731

1 Commander
Air Force Cambridge Research Laboratories
Attn: Data Sciences Lab
(Lt. S. J. Kahne, CRB)
L. G. Hanscom Field
Bedford, Massachusetts 01731

1 Commander
Air Force Systems Command
Office of the Chief Scientist
(Mr. A. G. Wimer)
Andrews AFB, Maryland 20331

1 Commander
Air Force Missile Development Center
Attn: MDSGO/Major Harold Wheeler, Jr.
Holloman Air Force Base, New Mexico

1 Commander
Research & Technology Division
Attn: MAYT (Mr. Evans)
Wright-Patterson Air Force Base
Ohio 45433

1 Directorate of Systems Dynamics Analysis
Aeronautical Systems Division
Wright-Patterson AFB, Ohio 45433

1 Hqs. Aeronautical Systems Division
AF Systems Command
Attn: Navigation & Guidance Laboratory
Wright-Patterson AFB, Ohio 45433

1 Commander
Rome Air Development Center
Attn: Documents Library, RAALD
Griffiss Air Force Base
Rome, New York 13442

1 Commander
Rome Air Development Center
Attn: RAWI-Major W. H. Harris
Griffiss Air Force Base
Rome, New York 13442

1 Lincoln Laboratory
Massachusetts Institute of Technology
P. O. Box 73
Lexington 73, Massachusetts
Attn: Library A-082

Continued next page

Distribution list as of March 1, 1965 (Cont'd.)

1 Lincoln Laboratory
Massachusetts Institute of Technology
P. O. Box 73
Lexington 73, Massachusetts
Attn: Dr. Robert Kingston

1 APGC (PGAPI)
Eglin Air Force Base
Florida

1 Mr. Alan Barnum
Rome Air Development Center
Griffiss Air Force Base
Rome, New York 13442

1 Director
Research Laboratory of Electronics
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

1 Polytechnic Institute of Brooklyn
55 Johnson Street
Brooklyn, New York 11201
Attn: Mr. Jerome Fox
Research Coordinator

1 Director
Columbia Radiation Laboratory
Columbia University
538 West 120th Street
New York, New York 10027

1 Director
Coordinated Science Laboratory
University of Illinois
Urbana, Illinois 61803

1 Director
Stanford Electronics Laboratories
Stanford University
Stanford, California

1 Director
Electronics Research Laboratory
University of California
Berkeley 4, California

1 Professor A. A. Dougal, Director
Laboratories for Electronics and Related
Science Research
University of Texas
Austin, Texas 78712

1 Professor J. K. Aggarwal
Department of Electrical Engineering
University of Texas
Austin, Texas 78712

1 Director of Engineering & Applied Physics
210 Pierce Hall
Harvard University
Cambridge, Massachusetts 02138

1 Capt. Paul Johnson (USN Ret.)
National Aeronautics & Space Agency
1520 H. Street, N. W.
Washington 25, D. C.

1 NASA Headquarters
Office of Applications
400 Maryland Avenue, S.Q.
Washington 25, D. C.
Attn: Code FC Mr. A. M. Greg Andrus

1 National Bureau of Standards
Research Information Center and Advisory
Serv. on Info. Processing
Data Processing Systems Division
Washington 25, D. C.

1 Dr. Wallace Sinaiko
Institute for Defense Analyses
Research & Eng. Support Div.
1666 Connecticut Avenue, N. W.
Washington 9, D. C.

1 Data Processing Systems Division
National Bureau of Standards
Conn. at Van Ness
Room 239, Bldg. 10
Washington 25, D. C.
Attn: A. K. Smilow

1 Exchange and Gift Division
The Library of Congress
Washington 25, D. C.

1 Dr. Alan T. Waterman, Director
National Science Foundation
Washington 25, D. C.

1 H. E. Cochran
Oak Ridge National Laboratory
P. O. Box X
Oak Ridge, Tennessee

1 U. S. Atomic Energy Commission
Office of Technical Information Extension
P. O. Box 62
Oak Ridge, Tennessee

1 Mr. G. D. Watson
Defense Research Member
Canadian Joint Staff
2450 Massachusetts Avenue, N. W.
Washington 8, D. C.

1 Martin Company
P. O. Box 5837
Orlando, Florida
Attn: Engineering Library MP-30

1 Laboratories for Applied Sciences
University of Chicago
6220 South Drexel
Chicago, Illinois 60637

1 Librarian
School of Electrical Engineering
Purdue University
Lafayette, Indiana

1 Donald L. Epley
Dept. of Electrical Engineering
State University of Iowa
Iowa City, Iowa

1 Instrumentation Laboratory
Massachusetts Institute of Technology
68 Albany Street
Cambridge 39, Massachusetts
Attn: Library WI-109

1 Sylvania Electric Products, Inc.
Electronics System
Waltham Labs. Library
100 First Avenue
Waltham 54, Massachusetts

2 Hughes Aircraft Company
Centinela and Teale Streets
Culver City, California
Attn: K. C. Rosenberg, Supervisor
Company Technical Document Center

3 Autonetics
9150 East Imperial Highway
Downey, California
Attn: Tech. Library, 3041-11

1 Dr. Arnold T. Nordsieck
General Motors Corporation
Defense Research Laboratories
6767 Hollister Avenue
Goleta, California

1 University of California
Lawrence Radiation Laboratory
P. O. Box 808
Livermore, California

1 Mr. Thomas L. Hartwick
Aerospace Corporation
P. O. Box 95085
Los Angeles 45, California

1 Lt. Col. Willard Levin
Aerospace Corporation
P. O. Box 95085
Los Angeles 45, California

1 Sylvania Electronic Systems-West
Electronic Defense Laboratories
P. O. Box 205
Mountain View, California
Attn: Documents Center

1 Varian Associates
611 Hansen Way
Palo Alto, California 94303
Attn: Tech. Library

1 Huston Denslow
Library Supervisor
Jet Propulsion Laboratory
California Institute of Technology
Pasadena, California

1 Professor Nicholas George
California Institute of Technology
Electrical Engineering Department
Pasadena, California

1 Space Technology Labs., Inc.
One Space Park
Redondo Beach, California
Attn: Acquisitions Group
STL Technical Library

1 The Rand Corporation
1700 Main Street
Santa Monica, California
Attn: Library

1 Miss F. Cloak
Radio Corp. of America
RCA Laboratories
David Sarnoff Research Center
Princeton, New Jersey

1 Mr. A. A. Lundstrom
Bell Telephone Laboratories
Room 2E-127
Whippany Road
Whippany, New Jersey

1 Cornell Aeronautical Laboratory, Inc.
4455 Genesee Street
Buffalo 21, New York
Attn: J. P. Desmond, Librarian

1 Sperry Gyroscope Company
Marine Division Library
155 Glenn Cove Road
Carle Place, L. I., New York
Attn: Miss Barbara Judd

1 Library
Light Military Electronics Dept.
General Electric Company
Armament & Control Products Section
Johnson City, New York

1 Dr. E. Howard Holt
Director
Plasma Research Laboratory
Rennselaer Polytechnic Institute
Troy, New York

1 Battele-DEFENDER
Battelle Memorial Institute
505 King Avenue
Columbus 1, Ohio

1 Laboratory for Electroscience Research
New York University
University Heights
Bronx 53, New York

1 National Physical Laboratory
Teddington, Middlesex
England
Attn: Dr. A. M. Uttley, Superintendent,
Autonomics Division

1 Dr. Lee Huff
Behavioral Sciences
Advanced Research Projects Agency
The Pentagon (Room 3E175)
Washington, D. C. 20301

1 Dr. Glenn L. Bryan
Head, Personnel and Training Branch
Office of Naval Research
Navy Department
Washington, D. C. 20360

1 Instituto de Fisica Aplicado
"L. Torres Quevedo"
High Vacuum Laboratory
Madrid, Spain
Attn: Jose L. de Segovia

1 Stanford Research Institute
Attn: G-037 External Reports
(for J. Goldberg)
Menlo Park, California 94025

REVISED U. S. ARMY DISTRIBUTION LIST

(As received at the Coordinated Science Laboratory 27 July 1965)

1 Dr. Chalmers Sherwin
Deputy Director (Research & Technology)
DD&RE Rm 3E1060
The Pentagon
Washington, D. C. 20301

1 Dr. Edward M. Reilley
Asst. Director (Research)
Ofc. of Defense Res. & Eng.
Department of Defense
Washington, D. C. 20301

1 Dr. James A. Ward
Office of Deputy Director (Research and Information Rm 3D1037)
Department of Defense
The Pentagon
Washington, D. C. 20301

1 Director
Advanced Research Projects Agency
Department of Defense
Washington, D. C. 20301

1 Mr. E. I. Salkovitz, Director for Materials Sciences
Advanced Research Projects Agency
Department of Defense
Washington, D. C. 20301

1 Colonel Charles C. Mack
Headquarters
Defense Communications Agency (333)
The Pentagon
Washington, D. C. 20305

20 Defense Documentation Center
Attn: TISIA
Cameron Station, Building 5
Alexandria, Virginia 22314

1 Director
National Security Agency
Attn: Librarian C-332
Fort George G. Meade, Maryland 20755

1 U. S. Army Research Office
Attn: Physical Sciences Division
3045 Columbia Pike
Arlington, Virginia 22204

1 Chief of Research and Development
Headquarters, Department of the Army
Attn: Mr. L. H. Geiger, Rm 3D442
Washington, D. C. 20310

1 Research Plans Office
U. S. Army Research Office
3045 Columbia Pike
Arlington, Virginia 22204

1 Commanding General
U. S. Army Materiel Command
Attn: AMCRD-RS-PE-E
Washington, D. C. 20315

1 Commanding General
U. S. Army Strategic Communications Command
Washington, D. C. 20315

1 Commanding Officer
U. S. Army Materials Research Agency
Watertown Arsenal
Watertown, Massachusetts 02172

1 Commanding Officer
U. S. Army Ballistics Research Laboratory
Attn: V. W. Richards
Aberdeen Proving Ground
Aberdeen, Maryland 21005

1 Commanding Officer
U. S. Army Ballistics Research Laboratory
Attn: Keats A. Pullen, Jr.
Aberdeen Proving Ground
Aberdeen, Maryland 21005

1 Commanding Officer
U. S. Army Ballistics Research Laboratory
Attn: George C. Francis, Computing Lab.
Aberdeen Proving Ground, Maryland 21005

1 Commandant
U. S. Army Air Defense School
Attn: Missile Sciences Division, C&S Dept.
P. O. Box 9390
Fort Bliss, Texas 79916

1 Commanding General
U. S. Army Missile Command
Attn: Technical Library
Redstone Arsenal, Alabama 35809

1 Commanding General
Frankford Arsenal
Attn: SMUFA-1310 (Dr. Sidney Ross)
Philadelphia, Pennsylvania 19137

1 Commanding General
Frankford Arsenal
Attn: SMUFA-1300
Philadelphia, Pennsylvania 19137

1 U. S. Army Munitions Command
Attn: Technical Information Branch
Picatinney Arsenal
Dover, New Jersey 07801

1 Commanding Officer
Harry Diamond Laboratories
Attn: Mr. Berthold Altman
Connecticut Avenue and Van Ness St.,N.W.
Washington, D. C. 20438

1 Commanding Officer
Harry Diamond Laboratories
Attn: Library
Connecticut Avenue and Van Ness St.,N.W.
Washington, D. C. 20438

1 Commanding Officer
U. S. Army Security Agency
Arlington Hall
Arlington, Virginia 22212

1 Commanding Officer
U. S. Army Limited War Laboratory
Attn: Technical Director
Aberdeen Proving Ground
Aberdeen, Maryland 21005

1 Commanding Officer
Human Engineering Laboratories
Aberdeen Proving Ground, Maryland 21005

1 Director
U. S. Army Engineer Geodesy, Intelligence & Mapping
Research and Development Agency
Fort Belvoir, Virginia 22060

1 Commandant
U. S. Army Command and General Staff College
Attn: Secretary
Fort Leavenworth, Kansas 66207

1 Dr. H. Robl, Deputy Chief Scientist
U. S. Army Research Office (Durham)
Box CM, Duke Station
Durham, North Carolina 27706

1 Commanding Officer
U. S. Army Research Office (Durham)
Attn: CRD-AA-IP (Richard O. Ulsh)
Box CM, Duke Station
Durham, North Carolina 27706

1 Superintendent
U. S. Army Military Academy
West Point, New York 10996

1 The Walter Reed Institute of Research
Walter Reed Army Medical Center
Washington, D. C. 20012

1 Commanding Officer
U. S. Army Electronics R&D Activity
Fort Huachuca, Arizona 85163

1 Commanding Officer
U. S. Army Engineers R&D Laboratory
Attn: STINFO Branch
Fort Belvoir, Virginia 22060

1 Commanding Officer
U. S. Army Electronics R&D Activity
White Sands Missile Range, New Mexico 88002

1 Director
Human Resources Research Office
The George Washington University
300 N. Washington Street
Alexandria, Virginia 22300

1 Commanding Officer
U. S. Army Personnel Research Office
Washington, D. C.

1 Commanding Officer
U. S. Army Medical Research Laboratory
Fort Knox, Kentucky 40120

1 Commanding General
U. S. Army Signal Center and School
Fort Monmouth, New Jersey 07703
Attn: Chief, Office of Academic Operations

1 Dr. S. Benedict Levin, Director
Institute for Exploratory Research
U. S. Army Electronics Command
Fort Monmouth, New Jersey 07703

1 Director
Institute for Exploratory Research
U. S. Army Electronics Command
Attn: Mr. Robert O. Parker, Executive Secretary, JSTAC (AMSEL-XL-D)
Fort Monmouth, New Jersey 07703

1 Commanding General
U. S. Army Electronics Command
Fort Monmouth, New Jersey 07703

Attn: AMSEL-SC
RD-D
RD-G
RD-MAF-I
RD-MAT
RD-GF
RD-MN (Marine Corps LnO)
XL-D
XL-E
XL-C
XL-S
HL-D
HL-L
HL-J
HL-P
HL-O
HL-R
NL-D
NL-A
NL-P
NL-R
NL-S
KL-D
KL-E
KL-S
KL-T
VL-D
WL-D

1 Mr. Charles F. Yost
Special Assistant to the Director of Research
National Aeronautics & Space Admin.
Washington, D. C. 20546

1 Director
Research Laboratory of Electronics
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

1 Polytechnic Institute of Brooklyn
55 Johnson Street
Brooklyn, New York 11201
Attn: Mr. Jerome Fox
Research Coordinator

1 Director
Columbia Radiation Laboratory
Columbia University
538 West 120th Street
New York, New York 10027

1 Director
Stanford Electronics Laboratories
Stanford University
Stanford, California 94301

1 Director
Electronics Research Laboratory
University of California
Berkeley, California 94700

1 Director
Electronic Sciences Laboratory
University of Southern California
Los Angeles, California 90007

1 Professor A. A. Dougal, Director
Laboratories for Electronics and Related Science Research
University of Texas
Austin, Texas 78712

1 Professor J. K. Aggarwal
Department of Electrical Engineering
University of Texas
Austin, Texas 78712

1 Division of Engineering and Applied Physics
210 Pierce Hall
Harvard University
Cambridge, Massachusetts 02138

Security Classification

DOCUMENT CONTROL DATA R&D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author)
University of Illinois
Coordinated Science Laboratory
Urbana, Illinois 61801

2a. REPORT SECURITY CLASSIFICATION
Unclassified

2b. GROUP

3. REPORT TITLE
A THEOREM ON THE MINIMUM DISTANCE OF BCH CODES OVER GF(q)

4. DESCRIPTIVE NOTES (Type of report and inclusive dates)

5. AUTHOR(S) (Last name, first name, initial)
Lum, Vincent

6. REPORT DATE
March, 1966

7a TOTAL NO. OF PAGES
19

7b. NO. OF REFS.
4

8a. CONTRACT OR GRANT NO.
DA 28 043 AMC 00073(E)

b. PROJECT NO.
20014501B31F

c. Also National Science Foundation Grant NSF GK-690

d.

9a. ORIGINATOR'S REPORT NUMBER(S)
R-281

9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)

10. AVAILABILITY/LIMITATION NOTICES
Qualified requesters may obtain copies of this report from DDC.
May be released to OTS.

11. SUPPLEMENTARY NOTES

12. SPONSORING MILITARY ACTIVITY
U. S. Army Electronics Command
Fort Monmouth, New Jersey 07703

13. ABSTRACT

This paper presents a generalization of Mattson-Soloman method for finding the minimum distance of a class of BCH codes. The theorem derived makes it possible to determine fairly easily if a particular code over GF(q) satisfies the conditions set forth and hence has minimum distance exceeding the BCH bound. Application of the theorem is given and numerous examples are presented.

DD FORM 1 JAN 64 1473

Security Classification

Security Classification

KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Mattson-Soloman method minimum distance BCH codes						

INSTRUCTIONS

1. ORIGINATING ACTIVITY: Enter the name and address of the contractor, subcontractor, grantee, Department of Defense activity or other organization (corporate author) issuing the report.

2a. REPORT SECURITY CLASSIFICATION: Enter the overall security classification of the report. Indicate whether "Restricted Data" is included. Marking is to be in accordance with appropriate security regulations.

2b. GROUP: Automatic downgrading is specified in DoD Directive 5200.10 and Armed Forces Industrial Manual. Enter the group number. Also, when applicable, show that optional markings have been used for Group 3 and Group 4 as authorized.

3. REPORT TITLE: Enter the complete report title in all capital letters. Titles in all cases should be unclassified. If a meaningful title cannot be selected without classification, show title classification in all capitals in parenthesis immediately following the title.

4. DESCRIPTIVE NOTES: If appropriate, enter the type of report, e.g., interim, progress, summary, annual, or final. Give the inclusive dates when a specific reporting period is covered.

5. AUTHOR(S): Enter the name(s) of author(s) as shown on or in the report. Enter last name, first name, middle initial. If military, show rank and branch of service. The name of the principal author is an absolute minimum requirement.

6. REPORT DATE: Enter the date of the report as day, month, year; or month, year. If more than one date appears on the report, use date of publication.

7a. TOTAL NUMBER OF PAGES: The total page count should follow normal pagination procedures, i.e., enter the number of pages containing information.

7b. NUMBER OF REFERENCES: Enter the total number of references cited in the report.

8a. CONTRACT OR GRANT NUMBER: If appropriate, enter the applicable number of the contract or grant under which the report was written.

8b, 8c, & 8d. PROJECT NUMBER: Enter the appropriate military department identification, such as project number, subproject number, system numbers, task number, etc.

9a. ORIGINATOR'S REPORT NUMBER(S): Enter the official report number by which the document will be identified and controlled by the originating activity. This number must be unique to this report.

9b. OTHER REPORT NUMBER(S): If the report has been assigned any other report numbers (either by the originator or by the sponsor), also enter this number(s).

10. AVAILABILITY/LIMITATION NOTICES: Enter any limitations on further dissemination of the report, other than those imposed by security classification, using standard statements such as:

(1) "Qualified requesters may obtain copies of this report from DDC."

(2) "Foreign announcement and dissemination of this report by DDC is not authorized."

(3) "U. S. Government agencies may obtain copies of this report directly from DDC. Other qualified DDC users shall request through

_____."

(4) "U. S. military agencies may obtain copies of this report directly from DDC. Other qualified users shall request through

_____."

(5) "All distribution of this report is controlled. Qualified DDC users shall request through

_____."

If the report has been furnished to the Office of Technical Services, Department of Commerce, for sale to the public, indicate this fact and enter the price, if known.

11. SUPPLEMENTARY NOTES: Use for additional explanatory notes.

12. SPONSORING MILITARY ACTIVITY: Enter the name of the departmental project office or laboratory sponsoring (paying for) the research and development. Include address.

13. ABSTRACT: Enter an abstract giving a brief and factual summary of the document indicative of the report, even though it may also appear elsewhere in the body of the technical report. If additional space is required, a continuation sheet shall be attached.

It is highly desirable that the abstract of classified reports be unclassified. Each paragraph of the abstract shall end with an indication of the military security classification of the information in the paragraph, represented as (TS), (S), (C), or (U).

There is no limitation on the length of the abstract. However, the suggested length is from 150 to 225 words.

14. KEY WORDS: Key words are technically meaningful terms or short phrases that characterize a report and may be used as index entries for cataloging the report. Key words must be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location, may be used as key words but will be followed by an indication of technical context. The assignment of links, roles, and weights is optional.

DD FORM 1 JAN 64 1473